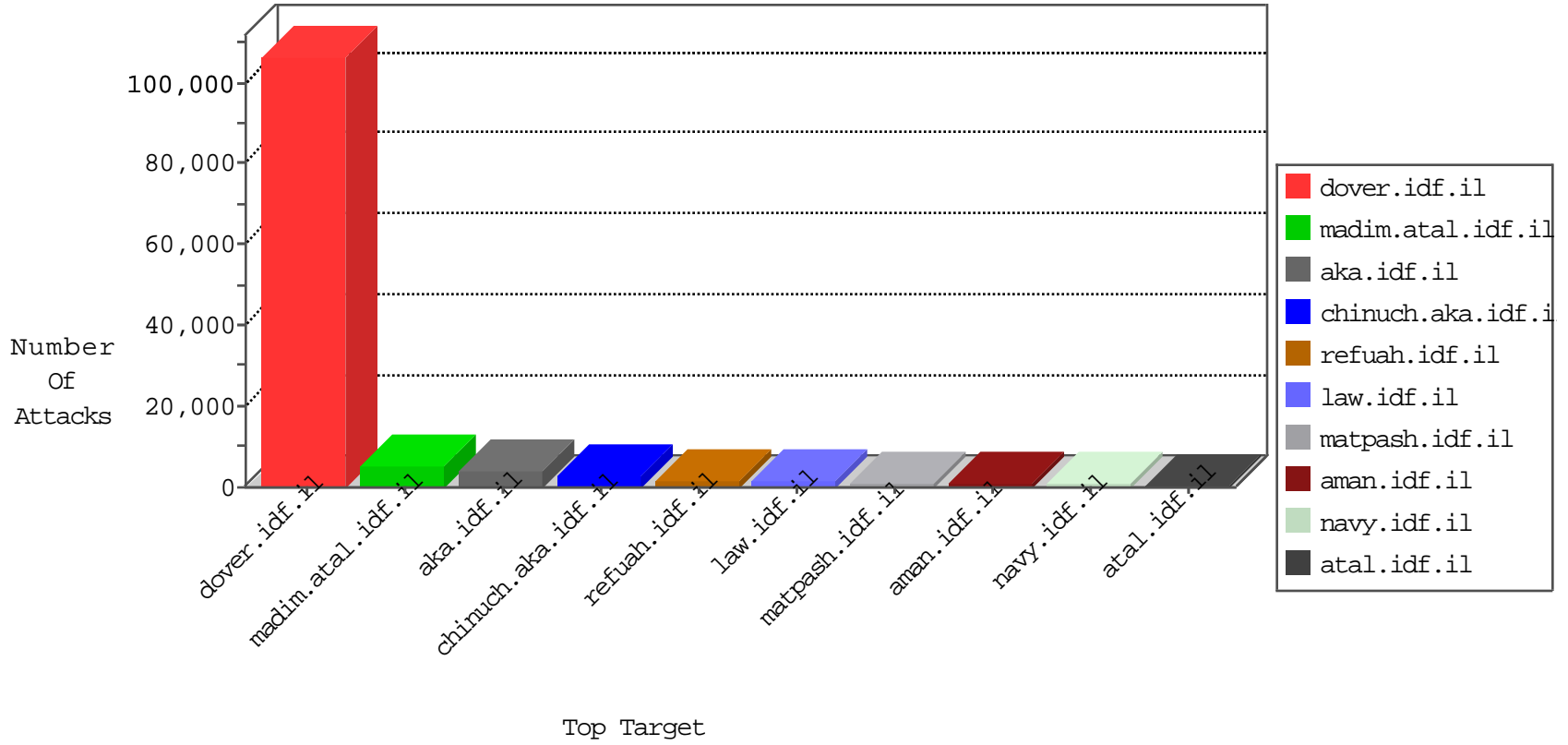


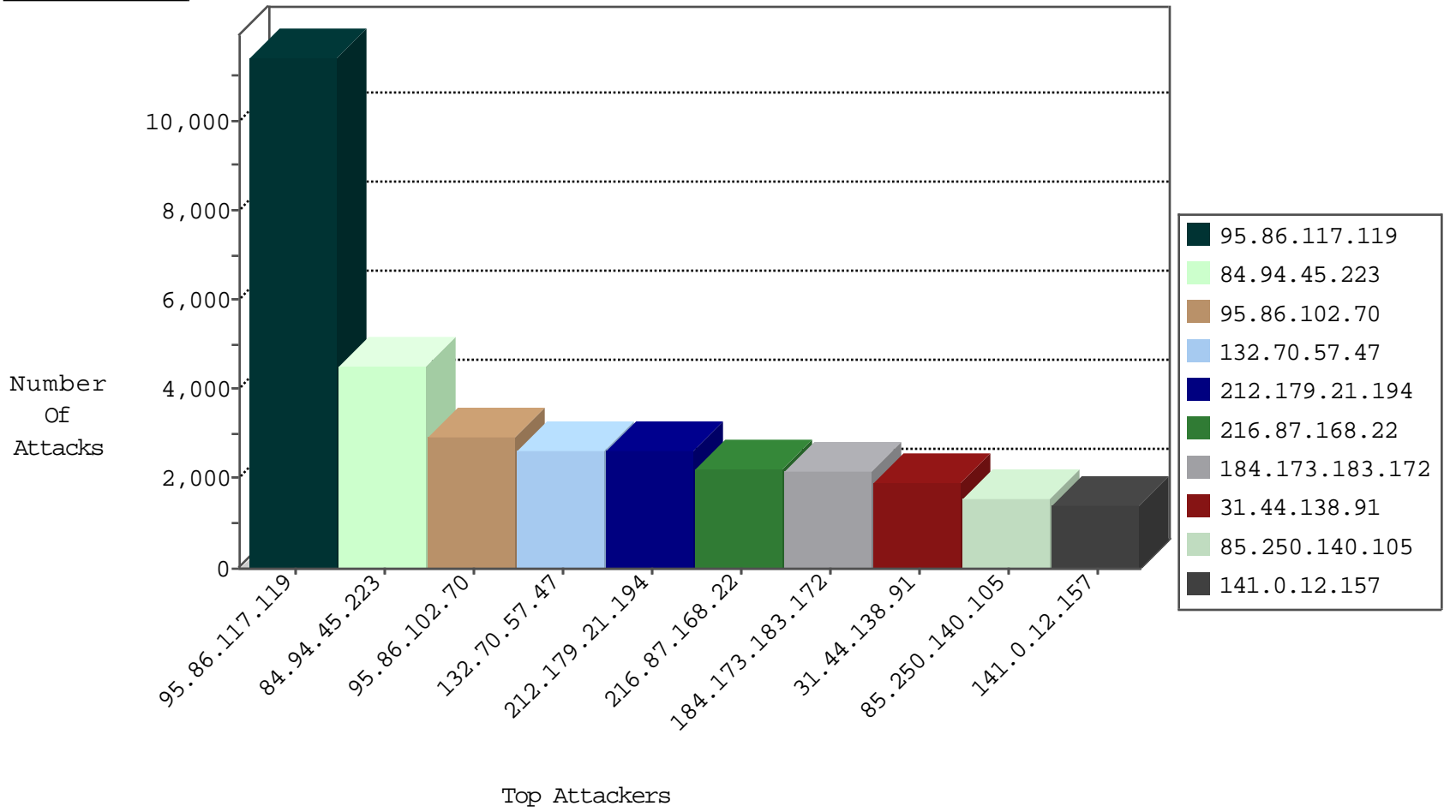
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	16367
216.87.168.22	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	14841
216.87.168.22	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	6269
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5878
216.87.168.22	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5707
66.249.69.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3338
109.253.136.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3005
46.117.107.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2747
180.87.253.58	India	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2567
79.176.125.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1234
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1228
66.249.64.151	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1101
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	622
41.249.238.76	Morocco	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	613
149.88.11.163	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	577
95.86.102.70	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	473
66.249.75.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	401
5.29.75.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	364
84.108.132.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	351
84.110.86.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	348
220.181.108.123	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	323
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	318
192.114.105.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	317
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	317
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	305
109.64.9.4	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
37.142.248.4	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
5.28.151.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
220.181.108.181	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	215
79.179.0.97	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	213
82.166.22.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
79.182.31.216	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
193.109.199.243	United Kingdom	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	160
5.29.40.173	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
5.29.63.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
37.26.147.196	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
85.65.130.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
46.120.137.166	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
79.178.134.112	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
212.179.28.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
91.231.193.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
85.65.198.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
82.80.17.247	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
176.13.6.242	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
5.29.208.179	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.45.223	Israel	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	2727
84.94.45.223	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1818
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	841
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	721
66.249.16.211	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	328
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	311
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	192
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	131
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	103
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	40
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
79.182.145.131	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
62.90.35.105	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	10
182.254.145.229	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	10
112.210.108.108	Philippines	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
218.77.79.43	China	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.198	e.yochanan.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	9
218.77.79.43	China	147.237.76.34	yochanan.idf.il	DVRep_B-N_60_100	Block	9
114.76.133.115	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	7
202.151.30.6	Fiji	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
218.77.79.43	China	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	7
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	7
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	6
87.69.215.49	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	6
46.19.85.79	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	6
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	6
93.172.156.5	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.111	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
218.77.79.43	China	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	6

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	96
66.249.69.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	10
41.249.238.76	Morocco	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	7
66.249.78.148	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	6
66.249.75.60	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
43.255.188.130	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	3
199.203.59.121	Israel	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	3
185.11.144.186	Russian Federation	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	3
66.249.78.147	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	3
43.255.188.131	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.130	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.131	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
176.31.180.116	France	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
114.245.136.159	China	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
43.255.188.130	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.160	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
176.31.180.116	France	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
101.226.2.99	China	147.237.0.33	idf.il	ET SCAN NMAP -f -sS	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
176.31.180.116	France	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.81	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
91.224.132.118	Russian Federation	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.68	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
198.52.97.84	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
43.255.188.130	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
5.102.254.57	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
43.255.188.130	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
222.186.21.201	China	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.65.83	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.117.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11442
95.86.102.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2918
132.70.57.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2621
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2507
31.44.138.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1921
85.250.140.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1493
141.0.12.157	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1382
173.56.50.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1377
212.199.205.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1357
46.210.192.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1307
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1239
2.54.53.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1215
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1169
2.54.21.28	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1152
190.229.126.218	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1002
193.106.54.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	934
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	933
80.246.133.231	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	775
185.26.180.86	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	763
200.53.156.138	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	757
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	716
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	702
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	649
65.49.68.206	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	636
92.62.170.49	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	528
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	511
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	485
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	465
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	462
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	438
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	432
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	408
79.176.197.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	398
109.253.100.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	397
188.165.15.95	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	394
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	376
69.41.14.152	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	374
69.41.14.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	374
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	369
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	334
5.29.173.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	332
149.255.232.16	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	326
46.19.86.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	322
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	316
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	316
82.145.211.77	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	310
109.65.113.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	307
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	305
84.110.86.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	298
79.182.145.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	294

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.17.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	486
176.12.138.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	469
62.128.35.129	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 62.128.35.129	Block	388
2.54.161.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	307
109.253.141.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	301
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	246
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	243
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	232
176.12.144.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.144.38	Block	211
84.228.1.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	209
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	197
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.140	Block	188
109.253.156.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	167
2.54.2.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	145
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	129
37.26.146.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	94
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	94
109.253.38.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
185.32.178.251	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.251	Block	85
46.19.86.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
109.253.144.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
80.246.136.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
109.253.135.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
176.12.143.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	62
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	58
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	56
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	52
176.12.146.155	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.146.155	Block	44
109.253.138.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
200.53.156.138	Mexico	147.237.76.147	chimuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	41
109.253.136.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
31.168.143.10	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 31.168.143.10	Block	30
109.253.135.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
149.88.118.203	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 149.88.118.203	Block	25
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
176.12.147.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
5.9.45.155	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.9.45.155	Block	18
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	17
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	16
31.168.27.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.27.1	Block	13
109.253.134.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
79.183.96.186	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il//templates/opcontactus/govcaptchaimage.axd	Block	11
79.179.15.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
178.137.84.13	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	10
46.117.26.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
2.54.25.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10